Эшелонированная оборона

Универсальность и безопасность каналов технологической связи

Сергей РОМАНОВ,
директор департамента НИОКР

Василий ХАРЛАМОВ,
начальник отдела оборудования, к.т.н., ЗАО «Юнител Инжиниринг» (Москва)

ВВЕДЕНИЕ

Технологические каналы и сети связи являются составной частью систем релейной защиты (РЗ) и противоаварийной автоматики (ПА), телемеханики, автоматики и диспетчеризации.

Набор параметров, характеризующих свойства технологических каналов и сетей связи, в прошлом выглядел так:

- Время передачи.
- Надежность.
- Безопасность.

В настоящее время этот набор расширен введением требований по:

- Унификации – использованию одинакового оборудования, систем управления и протоколов, изначально не предназначенных для специальных целей.
- Информационной безопасности (ИБ) – обеспечению неискаженной передачи информации к правильному адресату и недопущению ее несанкционированного возникновения.

Реализация новых требований рассматривается независимо от их влияния на традиционные параметры технологических каналов.

Специалисты по корпоративной ИБ не имеют достаточных знаний о специфике оборудования и систем электроэнергетики, считают, что технологические сети изолированы не только от сетей общего пользования, но и от внутренних сетей предприятия, в них применяются специальное оборудование, программное обеспечение (ПО) и протоколы, и поэтому поразить технологические системы невозможно.

Ранее нормировка параметров надежности и безопасности выполнялась по отношению сигнал/шум/помеха или вероятности ошибок. Сегодня приходится учитывать механизмы воздействия на технологические системы, принимать меры как по унификации систем связи и ИБ, так и обеспечивать защиту от преднамеренного или случайного вмешательства. Особенно важно последнее, так как число технологических нарушений растет не из-за природных, а техногенных причин.

УГРОЗЫ ТЕХНОЛОГИЧЕСКОЙ СВЯЗИ

Унифицированная аппаратура и управляющее ПО

Место специального оборудования в технологических сетях связи заняли разработанные для операторов связи мультиплексоры и маршрутизаторы, часто построенные с использованием устаревших версий операционных систем (ОС) с широко известными уязвимостями. Для использования в электроэнергетике они оснащаются встраиваемыми специализированными модулями. Управляющее ПО реализовано на базе Windows или Linux/Unix с использованием протоколов Telnet и SNMP по Ethernet/IP.

В результате как локально, так и по каналам управления дистанционно, немедленно или отложено могут быть поражены:

- управляющее ПО, что наименее опасно, если не приводит к поражению технологических каналов;
- аппаратные и программные ядра оборудования: отказ, изменение функциональности или искажение информации (опасно, так как нарушит технологические каналы);
- специализированные для электроэнергетики модули: отказ, изменение конфигурации или формирование ложных управляющих воздействий, например в модулях устройств передачи аварийных сигналов и команд (УПАСК), что наиболее опасно, так как может привести к системным авариям.

В 2011–2012 годах обнаружены уязвимости в продуктах RuggedCom, SEL и др. В 2013 году продемонстрированы уязвимости платформы ABB FOX515.

Время устранения таких уязвимостей обычно превышает один-два года, или устранить их вообще невозможно из-за устаревших ОС и средств разработки.

Унифицированные решения ИБ

Рядовые задачи обеспечения ИБ отличаются от задач обеспечения ИБ в технологической зоне тем, что здесь важно не только не допустить искажения/поражения информации, но и обеспечить ее доставку с нормированным временем и надежностью.

Поскольку стандартные методы обеспечения ИБ, например ГОСТ Р 34.10 и ГОСТ Р 34.11, основаны на информационной избыточности, они негативно скажутся на скорости и надежности передачи технологического трафика. Особенно это критично для систем РЗА и ПА. Возникает противоречие требований ИБ и технологий реального времени.

Технологические каналы и протоколы в унифицированных системах

Унификация систем связи не позволяет использовать в них ряд специальных технических решений по построению/защите технологических каналов. Вместо этого производится адаптация унифицированных решений для нужд технологий реального времени, функционирующих из-за этого в более тяжелых условиях и часто неудовлетворительно.

Фактически 100% алгоритмов передачи команд РЗ и ПА подвержены воздействию преднамеренных помех с обычно низкой степенью устойчивости. Это касается не только аналоговых, но и цифровых каналов связи, меняются лишь механизмы воздействия. При этом в цифровых системах технологической зоны

используются модифицированные связные протоколы и стандарты, например, Ethernet – > IEC 61850 – не самое удачное решение с точки зрения технологии реального времени и ИБ.

Архитектура унифицированных сетей и каналов

На используемые в технологической зоне унифицированные решения распространяются специальные требования, например по резервированию. Несоответствие унифицированных и специальных требований приводит к умножению на два числа оптических трактов, мультиплексоров и т.д.

Невозможность разделения зон обслуживания и ответственности между службами технологической зоны и зоны корпоративной связи приводит к дополнительной установке для служб технологической зоны облегченных унифицированных решений технологической связи. Следствие – умножение всего уже на три при сохранении вероятности поражения со стороны зоны корпоративной связи технологической зоны.

УНИВЕРСАЛЬНОСТЬ И БЕЗОПАСНОСТЬ ВМЕСТО УНИФИКАЦИИ

ИБ как подход

ИБ в технологической зоне нужна не столько для защиты конфиденциальных данных, сколько для обеспечения непрерывности производственного процесса. Для этого надо перенести риски поражения из программно-сетьсвязной плоскости в плоскость физического уровня: физически разделить зоны корпоративной и технологической связи, сделать обязательным для совершения любого действия личное присутствие.

При этом сокращается аппаратное обеспечение – достаточно физически вывести из облака унифицированных решений сервисы технологической зоны.

В технологической зоне следует вернуться к принципам функционального резервирования, например, для РЗ использовать ДЗЛ и цифровую сеть вместе с КСЗ и УПАСК по ВЧ каналу.

Доступ из корпоративной зоны в технологическую для управления и, возможно, мониторинга должен быть заблокирован на физическом уровне.

В технологической зоне должны максимально использоваться однонаправленные связи. Широковещательная передача между устройствами и сетями с дистанционным управлением должна быть запрещена, так как приводит к легкому одновременному поражению всех зон унифицированной системы.

Поскольку одними из самых распространенных методов поражения унифицированных систем и сетей связи являются закладки и инсайд, в технологической зоне необходимо:

• работы проводить на выведенном оборудовании под надзором специалистов служб технологической зоны;

• иметь для работы с оборудованием отдельный порт, физически изолированный от других, причем при его активации для исключения поражения системы в целом все другие порты необходимо физически отключить;

• для исключения отложенных поражений запретить оборудованию иметь встроенные носители информации: диски и флэш, а еще лучше и ОС;

• оборудование должно уметь определять отказ унифицированной среды передачи и либо подключаться к другой исправной среде передачи, либо отключаться вообще.

Поскольку в технологической зоне без нарушения парадигмы РЗА и ПА использовать ГОСТ Р 34.10 и ГОСТ Р 34.11 затруднительно, необходимо модернизировать в интересах ИБ протоколы и способы передачи. Желательно создать динамический ситуационный словарь (в каждый момент времени может быть передана только определенная информация).

Универсальность как подход

Архитектурные решения должны зависеть от того, в интересах какой конкретно службы внутри технологической зоны создаются каналы или сети связи.

На межобъектовом уровне должно быть все равно, через какую среду/оборудование передавать информацию. Главное – обеспечить защиту от атак со стороны параллельно работающих сервисов, в идеале – использовать независимые среды передачи для каждого сервиса.

На внутриобъектовом уровне для каждого сервиса или службы необходимо создавать защищенные независимые кластеры и при необходимости связи с другими кластерами использовать только однонаправленные связи, межсетевые разделительные однонаправленные экраны или защитные модули на базе анализаторов трафика на соответствие заданному словарю. Экраны на границах каждого кластера и их групп создадут многоуровневую эшелонированную оборону.